

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Peng T. Ong	§	Group Art Unit: 2436
	§	
Serial No. 10/617,607	§	Examiner: Johnson, Carlton
	§	
Filed: July 11, 2003	§	Customer No.: 50170
	§	
For: Consolidation of User Directories	§	
	§	

**Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450**

ATTENTION: Board of Patent Appeals and Interferences

APPELLANT'S BRIEF (37 C.F.R. § 41.37)

This Appeal Brief is in furtherance of the Notice of Appeal filed February 22, 2010 (37 C.F.R. § 41.31).

The fees required under § 41.20(b)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying Fee Transmittal.

I. Real Party in Interest

The real party in interest in this appeal is the following party: International Business Machines Corporation or Armonk, New York.

II. Related Appeals and Interferences

With respect to other appeals and interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

III. Status of Claims

The status of the claims involved in this proceeding is as follows:

1. Claims canceled: 2, 8, 11-16, and 18-20
2. Claims withdrawing from consideration but not canceled: NONE
3. Claims pending: 1, 3-7, 9, 10, 17, and 21-31
4. Claims allowed: NONE
5. Claims rejected: 1, 3-7, 9, 10, 17, and 21-31

The claims on appeal are: claims 1, 3-7, 9, 10, 17, and 21-31

IV. Status of Amendments

No amendments to the application were filed subsequent to mailing of the Final Office Action.

V. Summary of Claimed Subject Matter

With regard to independent claim 1, a method, in a data processing system (e.g., see **Figure 6; page 11, paragraph [0029], line 1 to page 12, paragraph [0031], line 6**), for providing a system administrator with a view (e.g., **page 19, paragraph [0046], lines 8-14; Figure 7**) of a plurality of applications accessible by a user is provided (e.g., **page 19, paragraph [0046], lines 1-8**). The method comprises receiving, in the data processing system, in response to a coupling of a separate hardware security device (e.g., **SOCI device 120 in Figure 1; see also Figure 3 and pages 7-8, paragraph [0024]**) to the data processing system (e.g., **page 12, paragraph [0033], lines 9-15**), credential information for each application of the plurality of applications that the user uses (e.g., **page 15, paragraph [0036], lines 1-15**), from the separate hardware security device into an authentication credential container (e.g., **page 20, paragraph [0048], lines 1-6**) associated with the user (e.g., **page 17, paragraph [0040], lines 9-11; page 19, paragraph [0046], lines 1-3**). The method further comprises identifying, by the data processing system, the plurality of applications accessible by the user by examining the authentication credential container associated with the user (e.g., **page 19, paragraph [0046], lines 1-3**). The method also comprises generating, by the data processing system, a view of the plurality of applications accessible by the user (e.g., **page 19, paragraph [0046], lines 1-14; view generator module of IMS; see also view example shown in Figure 7**). The view is a consolidated user directory that contains user authentication information across the plurality of applications (e.g., **page 19, paragraph [0046], lines 6-8; see Figure 7**). Moreover, the method comprises displaying, by the data processing system, the view to the administrator (e.g., **page 20, paragraph [0049], lines 1-5**).

Regarding independent claim 17, a method, in a data processing system (e.g., see **Figure 6; page 11, paragraph [0029], line 1 to page 12, paragraph [0031], line 6**), for providing a

system administrator with a list of a plurality of applications accessible by a user together with any user names and passwords used in connection with those applications (**e.g., page 19, paragraph [0046], lines 8-14; Figure 7**), is provided. The method comprises receiving, in the data processing system, in response to a coupling of a separate hardware security device (**e.g., SOCI device 120 in Figure 1; see also Figure 3 and pages 7-8, paragraph [0024]**) to the data processing system (**e.g., page 12, paragraph [0033], lines 9-15**), credential information for each application of a plurality of applications that the user uses (**e.g., page 15, paragraph [0036], lines 1-15**), from the separate hardware security device into an authentication credential container (**e.g., page 20, paragraph [0048], lines 1-6**) associated with the user (**e.g., page 17, paragraph [0040], lines 9-11; page 19, paragraph [0046], lines 1-3**). The method further comprises identifying, by the data processing system, the plurality of applications accessible by the user and any user names and passwords used in connection with the plurality of applications by examining an authentication credential container associated with the user (**e.g., page 19, paragraph [0046], lines 1-3**). Moreover, the method comprises generating, by the data processing system, a list of the plurality of applications accessible by the user together with any user names and passwords used in connection with the plurality of applications (**e.g., page 19, paragraph [0046], lines 1-14; view generator module of IMS; see also view example shown in Figure 7**). In addition, the method comprises displaying, by the data processing system, the list to the administrator (**e.g., page 20, paragraph [0049], lines 1-5**).

With regard to independent claim 28, a computer program product comprising a computer recordable medium having a computer readable program recorded thereon is provided. The computer readable program, when executed on a data processing system (**e.g., see Figure 6; page 11, paragraph [0029], line 1 to page 12, paragraph [0031], line 6**), causes the data processing system to: (1) receive, in response to a coupling of a separate hardware security device (**e.g., SOCI device 120 in Figure 1; see also Figure 3 and pages 7-8, paragraph [0024]**) to the data processing system (**e.g., page 12, paragraph [0033], lines 9-15**), credential information for each application of the plurality of applications that the user uses (**e.g., page 15, paragraph [0036], lines 1-15**), from the separate hardware security device into an authentication credential container (**e.g., page 20, paragraph [0048], lines 1-6**) associated with the user (**e.g., page 17, paragraph [0040], lines 9-11; page 19, paragraph [0046], lines 1-3**); (2) identify the

plurality of applications accessible by the user by examining the authentication credential container associated with the user (e.g., page 19, paragraph [0046], lines 1-3); (3) generate a view of the plurality of applications accessible by the user (e.g., page 19, paragraph [0046], lines 1-14; view generator module of IMS; see also view example shown in Figure 7), wherein the view is a consolidated user directory that contains user authentication information across the plurality of applications (e.g., page 19, paragraph [0046], lines 6-8; see Figure 7); and (4) display the view to the administrator (e.g., page 20, paragraph [0049], lines 1-5).

VI. Grounds of Rejection to be Reviewed on Appeal

The grounds of rejection to be reviewed on appeal are as follows:

(1) the rejection of claims 1, 3-7, 9, 10, and 21-31 under 35 U.S.C. § 103(a) based on Schaeck et al. (U.S. Patent Application Publication No. 2003/0163513) in view of Delany et al. (U.S. Patent Application Publication No. 2002/0138763), and further in view of Cotte (U.S. Patent Application Publication No. 2004/0013132) and Yasuda et al. (U.S. Patent No. 7,114,075); and

(2) the rejection of claim 17 under 35 U.S.C. § 103(a) based on Schaeck, Cotte, and Yasuda.

VII. Argument

A. Rejection under 35 U.S.C. § 103(a); Claims 1, 3-7, 9, 10, and 21-31

The Final Office Action rejects claims 1, 3-7, 9, 10, and 21-31 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Schaeck et al. (U.S. Patent Application Publication No. 2003/0163513), in view of Delany et al. (U.S. Patent Application Publication No. 2002/0138763), Cotte (U.S. Patent Application Publication No. 2004/0013132), and further in view of Yasuda et al. (U.S. Patent No. 7,114,075). This rejection is respectfully traversed.

In rejecting claims under 35 U.S.C. § 103, "the examiner bears the initial burden of presenting a *prima facie* case of obviousness." *In re Rijckaert*, 9 F.3d 1531, 1532, 28 USPQ.2d

(BNA) 1955, 1956 (Fed. Cir. 1993). To present this *prima facie* case of obviousness, it is incumbent upon the examiner to establish a factual basis to support the legal conclusion of obviousness. See *In re Fine*, 837 F.2d 1071, 1073, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). In so doing, the examiner is expected to make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17, 148 USPQ 459, 467 (1966). The examiner must articulate reasons for the examiner's decision. *In re Lee*, 277 F.3d 1338, 1342, 61 USPQ2d 1430, 1434 (Fed. Cir. 2002). In particular, the examiner must show that there is a teaching, motivation, or suggestion of a motivation to combine references relied on as evidence of obviousness. *Id.* at 1343, 61 USPQ2d at 1433-34. That is, to present a *prima facie* case of obviousness, the Examiner must show that "there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1741 (2007). The examiner cannot simply reach conclusions based on the examiner's own understanding or experience - or on his or her assessment of what would be basic knowledge or common sense. Rather, the examiner must point to some concrete evidence in the record in support of these findings. *In re Zurko*, 258 F.3d 1379, 1386, 59 USPQ2d 1693, 1697 (Fed. Cir. 2001). Thus the examiner must not only assure that the requisite findings are made, based on evidence of record, but must also explain the reasoning by which the findings are deemed to support the examiner's conclusion.

1. Independent Claims 1 and 28

Independent claim 1, which is representative of rejected independent claim 28 with regard to similarly recited subject matter, reads as follows:

1. A method, in a data processing system, for providing a system administrator with a view of a plurality of applications accessible by a user, comprising:

receiving, in the data processing system, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user;

identifying, by the data processing system, the plurality of applications accessible by the user by examining the authentication credential container

associated with the user;

generating, by the data processing system, a view of the plurality of applications accessible by the user, wherein the view is a consolidated user directory that contains user authentication information across the plurality of applications; and

displaying, by the data processing system, the view to the administrator.
(emphasis added)

Applicant respectfully submits that neither Schaeck, Delany, Cotte, nor Yasuda, either alone or in combination, teach or provide any technical rationale to implement at least the features emphasized above in claim 1, or the similar features found in independent claim 28.

Schaeck

Schaeck is directed to a mechanism for providing role based views of business web portals. With the mechanism of Schaeck, an aggregated service is comprised of one or more software resources. A role-specific portlet for each role supported by a particular one of the software resources is provided. A linkage between the role-specific portlets and the roles of the particular software resources is provided. At run time, a user role corresponding to a user of the aggregated services is obtained and a corresponding one of the role-specific portlets is programmatically selected to thereby provide a role-specific view of the aggregated service. The mechanism further determines which of the software resources to invoke to position the user's entry point into the aggregated service and uses the obtained role to select a role specific view of the determined software resource.

While Schaeck teaches to aggregate portlets for a user into an aggregate portal page view (see Figure 7 of Schaeck), nowhere in Schaeck is there any teaching or technical rationale provided regarding implementing the features of "receiving, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user" as recited in claim 1. To the contrary, in Figure 7 of Schaeck it is clearly shown that the user is presented with available services, the user selects a service, and based on the user's role, portlets associated with the service are selected and combined into an aggregate portal page that is presented to the user. Schaeck provides no teaching or technical rationale regarding implementing a separate hardware

security device, let alone receiving credential information for each application of a plurality of applications that the user uses *from the separate hardware security device* in response to the separate hardware security device being coupled to a data processing system or receiving such credential information into *an authentication credential container associated with the user*.

Moreover, Schaeck does not teach that the view that is generated is a *consolidated user directory that contains user authentication information across a plurality of applications*. To the contrary, the “view” that is generated in Schaeck is a portal page that has the portlets for a selected service. There is no teaching or technical rationale provided in Schaeck to implement this portal page such that it contains user authentication information across a plurality of applications. To the contrary, as described in paragraph [0073] of Schaeck, the portlets provide different interfaces for different user roles. In paragraph [0081] Schaeck teaches that the user’s role is determined based on the user’s login information, but this does not teach or provide any technical rationale to implement the actual view that is generated in Schaeck to contain user authentication information *across a plurality of applications*.

Cotte

Cotte does not teach or provide any technical rationale regarding implementing these features either, whether Cotte is taken alone or in combination with Schaeck. Cotte is cited as alleged teaching a plurality of applications at paragraph [0116]. Cotte is directed to a multiprotocol communications environment. In paragraph [0116] of Cotte, all that is taught is that it is possible to access a telecommunications portal in order to retrieve data about different telecommunications web sites residing on that telecommunications portal in total. There is nothing in Cotte that teaches or provides any technical rationale to implement the specific features of claim 1 discussed above with regard to Schaeck, i.e. a separate hardware device that is coupled to a data processing system; receiving, in response to a coupling of the separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user; or a view that is generated is a consolidated user directory that contains user authentication information across a plurality of applications. Merely providing a telecommunications portal that provides

information about telecommunications web sites has nothing to do with identifying a plurality of applications that a user may access from a separate hardware security device in response to such a device being coupled to a data processing system or that a view that is presented is a consolidated user directory that contains user authentication information across the plurality of applications.

Delany

The Final Office Action admits that Shaeck does not teach a consolidated user directory (Final Office Action, page 8) or a complete listing of applications (Final Office Action, pages 8-9). The Final Office Action alleges that Cotte teaches a complete listing of applications in paragraph [0116] which has been addressed above and has been shown to not actually teach or provide any technical rationale to implement such a feature but instead simply a presentation of information about telecommunications web sites. The Final Office Action further alleges, at pages 8-9, that Delany discloses a consolidated user directory that contains user authentication information across a plurality of applications at paragraph [0113], lines 13-18 and paragraph [0129], lines 16-20 which read as follows:

[0113] With Group Manager 44, companies (or other entities) can allow individual users to do the following: (1) self-subscribe to and unsubscribe from groups, (2) view the groups that they are eligible to join or have joined, and (3) request subscription to groups that have access to the applications they need. Multi-step workflows can then define which users must obtain approval before being added to a group and which can be added instantly. Group Manager 44 also lets companies form dynamic groups specified by an LDAP filter. The ability to create and use dynamic groups is extremely valuable because it eliminates the administrative headache of continually keeping individual, static membership up-to-date. With dynamic group management features, users can be automatically added or removed if they meet the criteria specified by the LDAP filter. Dynamic groups also greatly enhance security since changes in user identities that disqualify someone from membership in a group are automatically reflected in the dynamic group membership.

[0129] When database manager 120 starts, it will read the directory server configuration file(s) and insert corresponding profile and agent objects to its internal tables for later reference. FIG. 3 shows database manager 120 in communication with profiles 122, 124, 126 and 128. Each profile corresponds to an agent. For example, profile 122 corresponds to agent 130, profile 124

corresponds to agent 132, profile 126 corresponds to agent 134, and profile 128 corresponds to agent 136. Each agent is associated with a connection manager and a data store. For example, agent 130 is associated with connection manager 140 and data store 36a. Agent 132 is associated with connection manager 142 and data store 36b. Agent 134 is associated with connection manager 144 and data store 36c. Agent 136 is associated with connection manager 146 and data store 36d. In one embodiment, each of the data stores are LDAP directory servers with LDAP directories. In other embodiments, one or more of the data stores are LDAP directories and one or more of the data stores are other types of data stores (e.g. SQL servers) or others. In further embodiments, none of the data stores are LDAP directories.

As discussed in Responses filed April 30, 2008 and June 18, 2008 (page 13), and the Appeal Brief filed December 4, 2008, these sections of Delany only teach that (1) with the Group Manager in Delany, a user may view the groups that they are eligible to join or have joined and request subscription to groups that have access to the applications they need; (2) groups may be created dynamically with an LDAP filter; (3) the database manager reads a configuration file and inserts profile and agent objects to its internal tables; and (4) each profile corresponds to an agent and each agent is associated with a connection manager and a data store which may be an LDAP directory server. Nothing in these sections, or any other sections, of Delany teach or provide any technical rationale to implement generating a view of the plurality of applications accessible by the user, wherein the view is a consolidated user directory that contains user authentication information across the plurality of applications. Moreover, nothing in Delany teaches or provides any technical rationale to implement the feature of receiving, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user.

Yasuda

The Office Action admits that the combination of Schaeck, Delany, and Cotte does not teach a separate hardware security device (see Final Office Action, page 9). However, the Final Office Action alleges that these features are taught by Yasuda.

Yasuda is directed to a user authentication apparatus in which an IC card is used that has authentication information for a user for a number of applications. As described in columns 6

and 7 of Yasuda, with the use of the IC card, a user supplies a PIN which is then compared, within the IC card, to a stored PIN. If the PINs match, the client computer is given access to the IC card. A list of application names stored in records of the memory unit of the IC card is requested by the client and the names are returned by the IC card (column 6, lines 62-67). The names may be displayed to the user who then selects a name from the list (column 7, lines 1-5). In response to the user's selection, the authentication information for the selected application name is retrieved and provided to the client computer which inserts it into a logon image (column 7, lines 6-31).

While Yasuda teaches an IC card that may store authentication information for applications accessible by a user, nowhere in Yasuda is there any teaching or technical rationale provided with regard to *credential information for each application in a plurality of applications* being received *in an authentication credential container of the data processing system* from the IC card of Yasuda. To the contrary, Yasuda only teaches providing the authentication information for a single application in response to a user selecting that single application from the list of application names provided. Yasuda does not teach an authentication credential container being provided in the client of Yasuda and does not teach that such an authentication credential container receives authentication information for a plurality of applications from a separate hardware device. All that Yasuda teaches is that authentication information for a single application is provided to the client which then inserts it into a logon image.

Moreover, nowhere in Yasuda is there any teaching or technical rationale provided to implement generating a view of the plurality of applications accessible by the user, wherein the view is a consolidated user directory *that contains user authentication information across the plurality of applications*. To the contrary, Yasuda merely teaches providing a list of application names and, in response to a user selecting a name from the list, providing the authentication information for that single application to the client such that the client may immediately insert it into a logon image. There is no view of a plurality of applications provided in Yasuda where the view contains a consolidated user directory that contains user authentication information across a plurality of applications. The listing of application names in Yasuda does not provide any view of authentication information across a plurality of applications.

Thus, none of the cited references teach or render obvious the features of claim 1 discussed above. Since none of the cited references teach or render obvious these features, any alleged combination of these references still would not result in these features being taught or rendered obvious. To the contrary, even if such a combination of teachings from the references were possible and one were somehow motivated to attempt such a combination, *arguendo*, the result still would not be the invention as recited in claim 1. To the contrary, the combination would be some concoction of a system in which portlets associated with a selected service are combined into an aggregate portal page for a user based on the user's role (Schaeck), a telecommunications portal through which data about different telecommunications web sites may be accessed (Cotte), a view of groups that users are eligible to join or have joined may be displayed (Delany), and names of applications a user may access are retrieved from a separate device, a user selection of an application is received, and authentication information for the selected application is automatically inserted into a logon process (Yasuda). The combination would not result in the specific features of claim 1 as emphasized above.

Moreover, one of ordinary skill in the art would not have found it obvious to combine these four different references and then take the necessary inventive leaps to arrive at the claimed invention. These four references are all directed to solving different problems and present solutions that are not compatible with each other. There is no reason why one of ordinary skill in the art would combine an aggregate portal page mechanism with a telecommunications portal mechanism, a mechanism for viewing groups that a user can join, or a mechanism for performing automatic logon using a separate device based on a selection of an application.

The motivations offered by the Examiner for the various combinations are all just statements as to some benefit that the additional reference being added to the combination provides. The additional reference already achieves such benefits without the need of the other references. For example, on page 8 of the Final Office Action, the Examiner alleges that it would be obvious to combine Schaeck with Delany is "to enable, within a consolidated view or a single source, the addition and removal of directory entry attributes of an existing group." This is just a statement as to what Delany's mechanism provides. This does not address the alleged combination. Where is there any "existing groups" in Schaeck such that the mechanism of Delany would benefit Schaeck by providing an alleged "consolidated view"? There is no addressing in the alleged motivation as to where in the primary reference there is any statement

as to a need for such a benefit. Moreover, there is no statement as to how exactly these teachings would somehow be combined with the other references. How would providing an alleged consolidated view of existing groups, as in Delany, be combined with an aggregate portlet page such as described in Schaeck? The Examiner does not address such questions because, in fact, the two references are not combinable and one of ordinary skill in the art would not be motivated to combine these references.

The same concerns are present with each of the alleged “motivations” offered by the Examiner for the addition of the Cotte and Yasuda references. For example, with regard to the addition of Cotte, the Examiner alleges that one would be motivated to combine Cotte with Schaeck and Delany to achieve “privacy, ease of use, and/or data communication capabilities, offered by available communications environments.” Again, this has nothing to do with why or how the specific teachings relied upon in Cotte would somehow be combined with teachings of Schaeck and Delany. To the contrary, it only provides some generic benefit achieved by the Cotte reference independent of Schaeck and Delany and has nothing to do with combining teachings from Cotte with the other references.

Similarly, with regard to the combination of Yasuda with the other three references, the Examiner alleges the combination would be motivated in order to allegedly improve “security of the authentication information in order to achieve a high level security.” The teachings of the other references that are used to allegedly teach the features of the claimed invention do not include any “authentication information” and thus, it is not clear why Yasuda would be added to improve the security of such authentication information. Yet again, this is merely a statement taken from the additional reference, Yasuda, and reproduced in the Final Office Action which does not address the actual alleged combination of teachings but is just a statement as to a benefit allegedly achieved by the additional reference independent of the other references. In other words, there is no addressing of where the other references indicate a need for the alleged benefit of the additional reference and there is no addressing how such teachings of the additional reference could somehow be integrated with the teachings of the other references.

The alleged “motivations” amount to just an arbitrarily selected sentence from the additional reference regarding some benefit the additional reference allegedly achieves. This is not sufficient to support a finding of obviousness. Thus, the Examiner has failed to meet the burden of establishing a prima facie case of obviousness. The examiner has not only failed to

assure that the requisite findings are made, based on the evidence of record, as discussed above, but also has failed to explain the reasoning by which the findings are deemed to support the examiner's conclusion or reasoning addressing the particular combination of teachings rather than some arbitrarily selected generic statement.

Furthermore, as noted above, even if such a combination were possible and one were somehow motivated to attempt such a combination, the result still would not be the specific features recited in claim 1, or the similar features of claim 28.

In response to these arguments above, the Examiner merely reiterates the position espoused in the rejection and cites the same portions of the references as allegedly teaching the features of claim 1 (see Final Office Action, pages 3-4. Merely reiterating the same position does not address the specific arguments presented by Appellant. Thus, the Examiner has failed to convincingly rebut Appellant's arguments and thus, Appellant's arguments are believed to be still applicable and compelling.

Thus, for at least the reasons set forth above, Appellant respectfully submits that none of the cited references, Schaeck, Cotte, Delany, and Yasuda, whether taken alone or in combination, teaches or provides any technical rationale to implement the features of independent claim 1, or the similar features found in independent claim 28. Claims 3-7, 9, 10, and 21-31 depend from claims 1 and 28, respectively, and thus, are distinguished over the alleged combination of Schaeck, Cotte, Delany, and Yasuda at least by virtue of their dependency. Accordingly, Applicant respectfully requests the Board of Patent Appeals and Interferences to overturn the rejection of claims 1, 3-7, 9, 10, and 21-31 under 35 U.S.C. § 103(a).

2. Dependent Claims

In addition to the above, the alleged combination of references fails to teach or provide any technical rationale to implement the specific additional features presented in the dependent claims as discussed hereafter.

a. Dependent Claim 3

With regard to claim 3, Applicant respectfully submits that none of the cited references, whether taken alone or in combination, teaches or provides any technical rationale to implement

removing access to an application from the plurality of the applications *by utilizing the view of the plurality of the applications accessible by the user*. Again, none of the cited references teach or provide any technical rationale to implement a view that is a consolidated user directory that contains user authentication information across the plurality of applications. Therefore, the references cannot possibly teach or provide any technical rationale to implement using such a view to remove access to an application.

The Final Office Action (page 10) alleges that these features are taught by Schaeck at paragraphs [0043] and [0068] with the exception of providing a complete listing of applications, which the Final Office Action again alleges is taught by Cotte. Paragraphs [0043] and [0068] of Schaeck only teach that a service may have a number of different views established for the service and users with particular roles are provided with different views of the service. There is nothing in these sections of Schaeck that teach or provide any technical rationale to implement anything regarding using a view that is a consolidated user directory to remove access to an application, as recited in claim 3. Moreover, none of the other cited references teach or provide any technical rationale to implement such features and thus, any alleged combination of these references still would not result in these features being taught or rendered obvious.

b. Dependent Claim 6

Since the cited references do not teach or provide any technical rationale to implement the features of claim 3 as noted above, the cited references further cannot teach or provide any technical rationale to implement the features of claim 6, with regard to the removing being performed automatically. As noted above, none of the references teach a consolidated view being used to remove access to an application, let alone doing so automatically. Thus, claim 6 is distinguished over the alleged combination of references both by virtue of the specific features recited in claim 6 and by virtue of the dependency of claim 6 from claim 3.

The Final Office Action alleges that Schaeck teaches these features at paragraphs [0043] and [0044]. Paragraph [0043] of Schaeck merely teaches providing role specific views for aggregated services based on the services relevant to a particular role. Paragraph [0044] refers to Figure 2 of Schaeck and discusses a presentation interface for interfacing with a user. Neither of

these paragraphs teach anything regarding using a view that is a consolidated user directory to remove access to an application, let alone doing so automatically. Furthermore, none of the other cited references teach or render such features obvious. Thus, any alleged combination of these references still would not result in the features of claim 6 being taught or rendered obvious.

c. Dependent Claim 4

Regarding claim 4, Appellant respectfully submits that none of the cited references, whether taken alone or in combination, teach or provide any technical rationale to implement creating a user account for a new application to be accessible by the user utilizing the generated view or injecting authentication information of the user account into the authentication credential container of the user. The Final Office Action (pages 11-12) again alleges that the view feature is taught by Schaeck at paragraphs [0043] and [0068], which have been addressed above. The Final Office Action further references paragraph [0052] of Schaeck which only teaches that a composition tool may be used to combine fine grain services with a larger more general service. This does not provide any further teaching or technical rationale relevant to the view feature of the claims.

With regard to the features of creating a user account for a new application using the view and injecting authentication information of the user account, the Final Office Action points to Delany, paragraphs [0108] and [0109] as allegedly teaching these features. While these paragraphs do mention the creation and deletion functions of user management, there is no teaching or technical rationale provided in Delany regarding implementing the specific feature of using a view that is a consolidated user directory that contains user authentication information across a plurality of applications to perform such creation or deletion or injecting authentication information into an authentication credential container of the user.

Thus, none of the cited references teach or render obvious such features. Therefore, any alleged combination of these references still would not result in these features being taught or rendered obvious.

d. Dependent Claims 5 and 7

Since the cited references do not teach or provide any technical rationale to implement the features of claim 4 as noted above, the cited references further cannot teach or provide any

technical rationale to implement the features of claims 5 and 7, with regard to the authentication credential container being stored at a server and the creation of the user account being performed either automatically or manually by an administrator. The Final Office Action alleges that the features of claims 5 and 7 are taught by Delany at paragraphs [0128] and [0129] and Schaeck at paragraph [0044]. Paragraph [0044] of Schaeck has been addressed above and shown to only teach a presentation interface for interfacing with a user as shown in Figure 2 of Schaeck and does not have anything to do with a credential container being stored at a server or the creation of a user account either automatically or manually by an administrator.

Paragraphs [0128] and [0129] of Delany read as follows:

[0128] FIG. 1 shows Identity Server 40 communicating with Directory Server 36. The system can also support multiple directory servers (or other types of data stores). FIG. 3 depicts an exemplary architecture for supporting multiple directory servers based on the notion of abstracting database objects and separating database clients from the actual database access functionalities. By doing so, clients can be implemented in a database independent fashion. Database manager 120 is the central place where all database clients interface to access the data stores. In one embodiment, there is one database manager 120 for all clients.

[0129] When database manager 120 starts, it will read the directory server configuration file(s) and insert corresponding profile and agent objects to its internal tables for later reference. FIG. 3 shows database manager 120 in communication with profiles 122, 124, 126 and 128. Each profile corresponds to an agent. For example, profile 122 corresponds to agent 130, profile 124 corresponds to agent 132, profile 126 corresponds to agent 134, and profile 128 corresponds to agent 136. Each agent is associated with a connection manager and a data store. For example, agent 130 is associated with connection manager 140 and data store 36a. Agent 132 is associated with connection manager 142 and data store 36b. Agent 134 is associated with connection manager 144 and data store 36c. Agent 136 is associated with connection manager 146 and data store 36d. In one embodiment, each of the data stores are LDAP directory servers with LDAP directories. In other embodiments, one or more of the data stores are LDAP directories and one or more of the data stores are other types of data stores (e.g. SQL servers) or others. In further embodiments, none of the data stores are LDAP directories.

While these sections of Delany mention multiple directory servers and the server storing entries corresponding to agents, there is nothing in these, or any other, sections of Delany regarding authentication credential container being stored at a server and the creation of the user account

being performed either automatically or manually by an administrator. Merely mentioning that entries can be stored in servers does not render obvious the specific features of claims 5 and 7.

Hence, neither Delany nor Schaeck, in actuality, teach or render obvious the features of claims 5 and 7. Furthermore, the other cited references, likewise, do not teach or render obvious such features. Therefore, any alleged combination of these references still would not result in these features being taught or rendered obvious.

e. Dependent Claim 9

Regarding claim 9, Applicant respectfully submits that none of the cited references, either alone or in combination, teach or provide any technical rationale to implement the feature of the authentication information being injected into a separate hardware security device. With regard to this feature, the Final Office Action (page 14) alleges that Schaeck teaches such a feature in paragraph [0052], lines 11-15. In actuality, paragraph [0052] of Schaeck merely describes how a dynamic runtime integration of web services is made possible by the Schaeck mechanism and may use a composition tool for aggregating new web services. There is nothing in paragraph [0052] of Schaeck that mentions anything regarding injecting authentication information into a separate hardware security device. Furthermore, none of the other cited references teach or render obvious such features. Thus, any alleged combination of the references still would not result in these features being taught or rendered obvious.

f. Dependent Claim 10

Regarding claim 10, Applicant respectfully submits that none of the cited references, either alone or in combination, teach or provide any technical rationale to implement removing individual user directories for each application of the plurality of the applications accessible by the user. The Final Office Action (pages 14-15) again points to paragraphs [0043] and [0068] of Schaeck and paragraphs [0108] and [0109] of Delany. The paragraphs of Schaeck cited by the Final Office Action are just as irrelevant to these features as they are to the other features previously discussed. As noted above, these paragraphs teach that a service may have a number of different views established for the service and users with particular roles are provided with different views of the service. They do not teach anything regarding removing individual user directories for each application of a plurality of applications accessible by a user.

With regard to the cited portions of Delany, while Delany mentions a deletion function of user management, there is no teaching or technical rationale provided in Delany regarding implementing the specific features of removing *individual user directories for each application of the plurality of the applications accessible by the user*. Furthermore, none of the other cited references teach or render obvious such features. Thus, any alleged combination of Schaeck and Delany with the other references still would not result in these features being taught or rendered obvious.

g. Dependent Claim 21

With regard to claim 21, Applicant respectfully submits that none of the cited references, either alone or in combination, teaches or provides any technical rationale to implement that the view comprises a list of keys employed by the user, wherein each entry in the list corresponds to a different key employed by the user, and wherein each entry identifies a type of the corresponding key and a serial number of the corresponding key. The Final Office Action (page 15) admits that Schaeck does not teach this feature, but alleges that Delany teaches these features in paragraphs [0361] and [0374]. First, as noted above, Delany does not teach the view recited in independent claim 1 as discussed above, this view being the view referenced in claim 21. Second, the cited sections of Delany teach that a certificate may include fields specifying a key algorithm, a public key value, and a certificate serial number (see Delany, paragraph [0361]). However, nowhere in Delany is there any teaching of a view that has a list of keys with each entry in the list corresponding to a different key employed by a user. Thus, even though Delany teaches a public key value, a key algorithm, and a certificate serial number, Delany fails to teach or provide any technical rationale to implement these other features of claim 21 which are also not taught or rendered obvious by the other cited references. Thus, any alleged combination of Delany with the other cited references still would not result in the specific features of claim 21 being taught or rendered obvious.

h. Dependent Claim 22

With regard to claim 22, Applicant respectfully submits that none of the cited references, either alone or in combination, teach or provide any technical rationale to implement the feature

that the view comprises a profile of the user detailing a role of the user, a name of the user, contact information for the user, and employment information for the user. The Final Office Action (page 16), alleges that these features are taught by Schaeck at paragraphs [0108] and [0109] because Schaeck teaches a user profile. While Schaeck may teach a user profile, this does not teach that the view, which is a consolidated user directory as recited in claim 1, comprises such a profile. Thus, the alleged combination of references still fails to teach or provide any technical rationale to implement the specific features of claim 22.

i. Dependent Claim 23

Regarding claim 23, Applicant respectfully submits that none of the cited references, either alone or in combination, teach or provide any technical rationale to implement the feature that the view comprises a list of certificate-enabled applications accessible by the user, wherein each entry in the list corresponds to a different certificate-enabled application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding certificate-enabled application. The Final Office Action (page 16) alleges that these features are taught by Schaeck in paragraphs [0043] and [0068]. Paragraph [0043] merely provides examples of a role specific view of a service. Paragraph [0068] merely describes the defining of separate role views for services. Neither of these portions of Schaeck, or any other portion of Schaeck, teaches or provides any technical rationale to implement the specific features of a list of certificate-enabled applications accessible by a user with entries in the list corresponding to different certificate enabled applications and each entry identifying a user name and a last login attempt of the user. These features are not even really addressed by the Final Office Action but instead are merely disregarded by pointing to the same general sections of Schaeck previously cited without any analysis as to how they apply to the specific features of the claim. There simply is no teaching in Schaeck, or any of the other cited references, regarding the specific features of claim 23. Thus, any alleged combination of Schaeck with the other cited references still would not result in the features of claim 23 being taught or rendered obvious.

j. Dependent Claim 24

Regarding claim 24, Applicant respectfully submits that none of the cited references, either alone or in combination, teach or provide any technical rationale to implement that the

view comprises a list of enterprise applications accessible by the user, wherein each entry in the list corresponds to a different enterprise application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding enterprise application.

Similar to the rejection of claim 23 above, the Final Office Action (page 17) cites the same sections of Schaeck as allegedly teaching these features but then further states that Delany teaches the last login attempt of the user feature at paragraphs [0428] and [0429]. These paragraphs of Delany generally teach the “logging” of successful and unsuccessful login attempts. However, there is no teaching or technical rationale provided in Delany, or the cited portions of Schaeck, regarding implementing a view, such as that recited in claim 1, and claim 24 by its dependency, having the entries for each enterprise application and these entries having the user name and last login attempt, as recited in claim 24. The specific arrangement of elements set forth in claim 24 is neither taught nor rendered obvious by the alleged combination of references.

k. Dependent Claim 25

Regarding claim 25, Applicant respectfully submits that none of the cited references, either alone or in combination, teach or provide any technical rationale to implement the feature that the view comprises a list of personal applications accessible by the user, wherein each entry in the list corresponds to a different personal application, and wherein each entry identifies a number of accounts connected to the corresponding personal application. The Final Office Action (pages 17-28) alleges that these features are taught by Schaeck in paragraphs [0043] and [0068] which have been addressed above. As noted above, these sections only discuss examples of different role views of a service and provide no teaching or technical rationale regarding implementing any list of personal applications, let alone such a list that has entries that correspond to different personal applications with each entry identifying a number of accounts connected to the personal application. There simply is no correlation between the paragraphs of Schaeck and the features of claim 25. Thus, any alleged combination of Schaeck with the other cited references still would not result in the features of claim 25 being taught or rendered obvious.

l. Dependent Claim 26

Regarding claim 26, Applicant respectfully submits that none of the cited references, either alone or in combination, teach or provide any technical rationale to implement the feature that the view comprises user selectable graphical user interface elements for invoking a function to update the profile and for invoking a function to reset the profile. The Final Office Action (page 18) points to paragraphs [0043], [0044], and [0066] of Schaeck as allegedly teaching these features. Paragraph [0043] provides examples of role based views of a service, paragraph [0044] teaches “user-facing” web applications having user interfaces for communicating with a user, and paragraph [0066] teaches the modification of user profiles. However, nowhere in Schaeck is there any teaching or technical rationale provided regarding implementing a view, such as that recited in claims 1 and 26, having selectable graphical user interface elements to update the profile portion of the view and for invoking a reset of the profile. Thus, any alleged combination of Schaeck with the other cited references still would not result in the features of claim 26 being taught or rendered obvious.

m. Dependent Claim 27

Regarding claim 27, Applicant respectfully submits that none of the cited references, either alone or in combination, teach or provide any technical rationale to implement that the view comprises a user selectable graphical user interface element for invoking a function to delete a user name of the user from the list of certificate-enabled applications. Again, the Final Office Action (page 18) points to paragraphs [0043], [0044], and [0066] as allegedly teaching these features. As noted above with regard to the rejection of claim 26, Schaeck in fact does not teach the specific features of claim 27 in a similar way that Schaeck does not teach the features of claim 26. While Schaeck may generally teach the modification of user profiles, Schaeck provides no teaching or technical rationale provided regarding implementing the specific arrangement of features set forth in claim 27. Thus, any alleged combination of Schaeck with the other cited references still would not result in the features of claim 27 being taught or rendered obvious.

n. Dependent Claims 29-31

Dependent claim 29 recites similar features to that of dependent claim 3. Dependent claim 30 recites similar features to that of dependent claim 23. Dependent claim 31 recites similar features to that of dependent claims 23-27 recited in the alternative. Thus, these claims are distinguished over the alleged combination of reference for similar reasons as noted above with regard to the similar claims.

B. Rejection under 35 U.S.C. § 103(a), Claim 17

The Final Office Action rejects claim 17 under 35 U.S.C. §103(a) as being allegedly unpatentable over Schaeck et al. in view of Cotte, and further in view of Yasuda. This rejection is respectfully traversed.

As discussed in the Responses filed April 30, 2008, June 18, 2008 (pages 10-12), and the Appeal Brief filed December 4, 2008, independent Claim 17 recites receiving, *in the data processing system*, in response to a coupling of a separate hardware security device to the data processing system, *credential information for each application of a plurality of applications* that the user uses from the separate hardware security device, *into an authentication credential container associated with the user*. As discussed at length above with regard to claim 1, neither Schaeck, Cotte nor Yasuda, either alone or in combination, teach or provide any technical rationale to implement such features.

As discussed above, in Figure 7 of Schaeck it is clearly shown that the user is presented with available services, the user selects a service, and based on the user's role, portlets associated with the service are selected and combined into an aggregate portal page that is presented to the user. Schaeck provides no teaching or technical rationale regarding implementing a separate hardware security device, let alone receiving credential information for each application of a plurality of applications that the user uses from the separate hardware security device in response to the separate hardware security device being coupled to a data processing system or receiving such credential information into an authentication credential container associated with the user.

Cotte likewise does not teach or provide any technical rationale regarding implementing these features either, whether Cotte is taken alone or in combination with Schaeck. As discussed

above, Cotte teaches that it is possible to access a telecommunications portal in order to retrieve data about different telecommunications web sites residing on that telecommunications portal in total. However, there is nothing in Cotte that teaches or provides any technical rationale to implement the specific features of claim 17 discussed above with regard to Schaeck, i.e. a separate hardware device that is coupled to a data processing system; receiving, ***in the data processing system***, in response to a coupling of the separate hardware security device to the data processing system, credential information ***for each application of the plurality of applications*** that the user uses from the separate hardware security device ***into an authentication credential container associated with the user***. Merely providing a telecommunications portal that provides information about telecommunications web sites has nothing to do with identifying a plurality of applications that a user may access from a separate hardware security device in response to such a device being coupled to a data processing system or that a view that is presented is a consolidated user directory that contains user authentication information across the plurality of applications.

Moreover, as discussed above, Yasuda, while teaching a separate hardware security device, i.e. the IC card, only teaches providing a single authentication information for a single application in response to a user selecting an application name from a list. Yasuda does not provide any teaching regarding an authentication credential container in a data processing system or receiving credential information for a plurality of applications from the IC card into the authentication credential container.

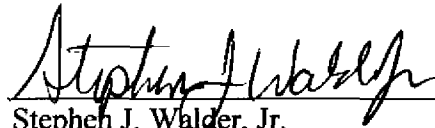
Furthermore, none of the cited references teach or provide any technical rationale to display a listing of a plurality of applications accessible by the user ***together with any user names and passwords used in connection with the plurality of applications***. To the contrary, all that Yasuda teaches is displaying a list of application names so that a user can select which application they want to access.

In view of the above, Applicant respectfully submits that neither Schaeck, Cotte, nor Yasuda, either alone or in combination, teaches or provides any technical rationale to implement the features of claim 17. Accordingly, Applicant respectfully requests that the Board of Patent Appeals and Interferences overturn the rejection of claim 17 under 35 U.S.C. § 103(a).

VIII. Conclusion

In view of the above, Appellant respectfully submits that claims 1, 3-7, 9, 10, 17, and 21-31 of the present application are directed to statutory subject matter and that the features of these claims are not taught or suggested by the Schaeck, Delany, Cotte, and Yasuda references. Accordingly, Appellant requests that the Board of Patent Appeals and Interferences overturn the rejections set forth in the Final Office Action.

Respectfully submitted,

A handwritten signature in black ink, reading "Stephen J. Walder, Jr.", is written over a horizontal line.

Stephen J. Walder, Jr.
Reg. No. 41,534

Walder Intellectual Property Law, P.C.
17330 Preston Road, Suite 100B
Dallas, TX 75252
(972) 380-9475
ATTORNEY FOR APPELLANT

CLAIMS APPENDIX

1. A method, in a data processing system, for providing a system administrator with a view of a plurality of applications accessible by a user, comprising:

receiving, in the data processing system, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses, from the separate hardware security device into an authentication credential container associated with the user;

identifying, by the data processing system, the plurality of applications accessible by the user by examining the authentication credential container associated with the user;

generating, by the data processing system, a view of the plurality of applications accessible by the user, wherein the view is a consolidated user directory that contains user authentication information across the plurality of applications; and

displaying, by the data processing system, the view to the administrator.

3. The method of claim 1 further comprising removing access to an application from the plurality of the applications by utilizing the view of the plurality of the applications accessible by the user.

4. The method of claim 1 further comprising:

creating a user account for a new application to be accessible by the user utilizing the generated view; and

injecting authentication information of the user account into the authentication credential container of the user.

5. The method of claim 4 wherein the authentication credential container is stored at a server.
6. The method of claim 3 wherein the removing is performed automatically.
7. The method of claim 4 wherein the creating the user account is performed either automatically or manually by an administrator.
9. The method of claim 4 wherein the authentication information is injected into the separate hardware security device.
10. The method of claim 1 further comprising removing individual user directories for each application of the plurality of the applications accessible by the user.
17. A method, in a data processing system, for providing a system administrator with a list of a plurality of applications accessible by a user together with any user names and passwords used in connection with those applications, comprising:
 - receiving, in the data processing system, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of a plurality of applications that the user uses, from the separate hardware security device into an authentication credential container associated with the user;
 - identifying, by the data processing system, the plurality of applications accessible by the user and any user names and passwords used in connection with the plurality of applications by

examining an authentication credential container associated with the user;

generating, by the data processing system, a list of the plurality of applications accessible by the user together with any user names and passwords used in connection with the plurality of applications; and

displaying, by the data processing system, the list to the administrator.

21. The method of claim 1, wherein the view comprises:

a list of keys employed by the user, wherein each entry in the list corresponds to a different key employed by the user, and wherein each entry identifies a type of the corresponding key and a serial number of the corresponding key.

22. The method of claim 1, wherein the view comprises:

a profile of the user detailing a role of the user, a name of the user, contact information for the user, and employment information for the user.

23. The method of claim 1, wherein the view comprises:

a list of certificate-enabled applications accessible by the user, wherein each entry in the list corresponds to a different certificate-enabled application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding certificate-enabled application.

24. The method of claim 1, wherein the view comprises:

a list of enterprise applications accessible by the user, wherein each entry in the list

corresponds to a different enterprise application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding enterprise application.

25. The method of claim 1, wherein the view comprises:

a list of personal applications accessible by the user, wherein each entry in the list corresponds to a different personal application, and wherein each entry identifies a number of accounts connected to the corresponding personal application.

26. The method of claim 22, wherein the view comprises:

user selectable graphical user interface elements for invoking a function to update the profile and for invoking a function to reset the profile.

27. The method of claim 23, wherein the view comprises:

a user selectable graphical user interface element for invoking a function to delete a user name of the user from the list of certificate-enabled applications.

28. A computer program product comprising a computer recordable medium having a computer readable program recorded thereon, wherein the computer readable program, when executed on a data processing system, causes the data processing system to:

receive, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses, from the separate hardware security device into an authentication credential container associated with the user;

identify the plurality of applications accessible by the user by examining the authentication credential container associated with the user;

generate a view of the plurality of applications accessible by the user, wherein the view is a consolidated user directory that contains user authentication information across the plurality of applications; and

display the view to the administrator.

29. The computer program product of claim 28, wherein the computer readable program further causes the data processing system to remove access to an application from the plurality of the applications by utilizing the view of the plurality of the applications accessible by the user.

30. The computer program product of claim 28, wherein the computer readable program further causes the data processing system to:

create a user account for a new application to be accessible by the user utilizing the generated view; and

inject authentication information of the user account into the authentication credential container of the user.

31. The computer program product of claim 28, wherein the view comprises at least one of:

a list of certificate-enabled applications accessible by the user, wherein each entry in the list corresponds to a different certificate-enabled application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding certificate-enabled application;

a list of enterprise applications accessible by the user, wherein each entry in the list corresponds to a different enterprise application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding enterprise application;

a list of personal applications accessible by the user, wherein each entry in the list corresponds to a different personal application, and wherein each entry identifies a number of accounts connected to the corresponding personal application;

user selectable graphical user interface elements for invoking a function to update the profile and for invoking a function to reset the profile; or

a user selectable graphical user interface element for invoking a function to delete a user name of the user from the list of certificate-enabled applications.

EVIDENCE APPENDIX

NONE

RELATED PROCEEDINGS APPENDIX

NONE